2 General Policy

2.1 What to Include

As described in the NIST Computer Security Handbook, a useful structure for issue-specific policy is to break the policy into its basic components.

Issue Statement. To formulate a policy on an issue, managers first must define the issue with any relevant terms, distinctions, and conditions included. It is also often useful to specify the goal or justification for the policy—which can be helpful in gaining compliance with the policy. For Internet security policy, an organization may need to be clear whether the policy covers all Internet-working connections or only Internet ones. The policy may also state whether other Internet non-security issues are addressed, such as personal use of Internet connections.

Statement of the Organization's Position. Once the issue is stated and related terms and conditions are discussed, this section is used to clearly state the organization's position (i.e., management's decision) on the issue. This would state whether Internet connectivity is allowed or not and under what conditions.

Applicability. Issue-specific policies also need to include statements of applicability. This means clarifying where, how, when, to whom, and to what a particular policy applies. Does this apply to all components of the organization? A public affairs type of office may be exempted from a restrictive policy.

Roles and Responsibilities. The assignment of roles and responsibilities is also needed. For a complex issue such as Internet security, technical roles to analyze the security of various architectures or management roles granting approvals may need to be defines. If a monitoring role may also be needed.

Compliance. For some types of Internet policies, it may be appropriate to describe, in some detail, the infractions that are unacceptable, and the consequences of such behavior. Penalties may be explicitly stated and should be consistent with organizational personnel policies and practices. When used, they should be coordinated with appropriate officials and offices and, perhaps, employee bargaining units. It may also be desirable to task a specific office within the organization to monitor compliance.

Points of Contact and Supplementary Information. For any issue-specific policy, the appropriate individuals in the organization to contact for further information, guidance, and compliance should be indicated. Since positions tend to change less often than the people occupying them, specific positions may be preferable as the point of contact. For example, for some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, system administrator, or security program representative. Internet rules or system specific policies should be cited. (These are described in the next section of this book.)

2.2 Obtaining Approval

What is the Organization? Policy (good policy) can only be written for a defined group with similar goals. Therefore an organization may need to divide itself into components if the parent organization is too big or too diverse to be the subject of an Internet security policy. For example NIST is a component agency of the Department of Commerce (DOC). NIST's mission requires a large amount of scientific collaboration in an open environment. Another component of DOC, the Census Bureau, has a requirement to maintain the confidentiality of individual census questionnaires. With such different missions and requirements, a central Internet security policy from DOC is probably not needed. Even within NIST there are significant differences in mission and requirements such that most Internet security policy is set at a lower level than NIST-wide.

Ties to Other Policy Areas. The Internet is one of many ways in which a typical organization interacts with external sources. Internet policy should be consistent with other policy mediating access with the outside. For example:

Physical access to the organization's building(s) or campus. In one sense the Internet is an electronic doorway to the organization. Both good and bad things use the same doorway. An organization which has an open physical campus has, presumably, already made a risk-based decision that the openness is either essential for the organization's mission or that the threat is low or too expensive to mitigate. A similar logic may hold for an electronic door. However, there are important differences. Physical threats are more directly linked to physical location. Linking to the Internet is linking to the entire world. An organization whose physical plant is in a remote and friendly place, say Montana, might have an open physical campus, but still require a restrictive Internet policy.

Public/Media Interaction. The Internet can be a form of public dialogue. Many organizations instruct employees how to work with the public or the media. These policies will probably need to be ported to electronic interactions. Many employees may not be aware of the public nature of the Internet.

Electronic access. The Internet is not the only means of Internet-working. Organizations use the telephone system (public switched network) and other public and private networks to connect external users and computer systems to internal systems. Connecting to the Internet and the telephone system share some threats and vulnerabilities.

2.3 Getting Policy Implemented

Don't assume that just because your organization has a lot of policies or directives or internal regulations that that is how policy is set. Look around and see if any of the formal writings are followed. If not, you can either try to re-invent your organization's paperwork process (generally difficult, but perhaps worthwhile) or figure out where the policy is really set. (If you pick the second option you will probably also need the formal writing.)

Since, unfortunately, a study of informal policy is beyond the scope of this book, this very important piece of the process will not be well described. However, most policy is set by what the big boss really wants. For an organization's Internet security policy (or any policy) to be effective, the big boss has to understand the choice to be made and make it freely. Generally if the big boss believes the policy it will filter through the informal mechanisms.

Some Helpful Hints on Policy

To be effective, policy requires visibility. Visibility aids implementation of policy by helping to ensure policy is fully communicated throughout the organization. Management presentations, videos, panel discussions, guest speakers, question/answer forums, and newsletters increase visibility. The organization's computer security training and awareness program can effectively notify users of new policies. It also can be used to familiarize new employees with the organization's policies.

Computer security policies should be introduced in a manner that ensures that management's unqualified support is clear, especially in environments where employees feel inundated with policies, directives, guidelines, and procedures. The organization's policy is the vehicle for emphasizing management's commitment to computer security and making clear their expectations for employee performance, behavior, and accountability.

To be effective, policy should be consistent with other existing directives, laws, organizational culture, guidelines, procedures, and the organization's overall mission. It should also be integrated into and consistent with other organizational policies (e.g., personnel policies). One way to help ensure this is to coordinate policies during development with other organizational offices.

2.4 Sample High Level Policy Statements

This section provides some sample policies. It is not meant to preclude other formats, other levels of detail, but is meant to assist the reader understanding the principles laid out in this chapter.

The first is for an organization which chooses not to restrict Internet access in any way. While this course is fraught with many security perils, it may be the best choice for an organization which requires openness or requires a lack of control by management on the working level. In general these organizations are best advised to separate at least some data and processing from the main organization processing. For example, some universities and colleges need this kind of environment for student and faculty systems. (But not for administrative systems.)

The second example is more a middle-of-the-road policy. Internal and public systems are separated by a firewall. However, most Internet-based services are still made available to the internal users. Generally a dual-homed gateway or a bastion host would serve as the firewall. However, this approach can also be implemented through the use of cryptography to create virtual private networks or tunnels on the Internet.

The third example is for an organization that requires security more than Internet services. The only Internet service for which the organization sees a business case is email. It is interesting to note that one factor in the business case is to provide email as a perk for employees. The company still provides a public access server for the Internet, but it is not connected to internal systems.